UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,508	06/29/2001	James S. Magdych	NAII-P011/01.116.01	7235

28875 7590 03/01/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/895,508	MAGDYCH ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2001*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-6,9-12,15-17 and 20-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed December 22, 2004, have been fully considered but they are not persuasive.

Response to Amendment

2. The examiner approves the replacement sheet for figure 1 received on 22 December 2004. The examiner withdraws the objection to the drawings.

3. The examiner withdraws the rejection under 35 U.S.C. 101 to claims 12-22, 26.

4. Applicant states that Shostack et al. merely makes a blanket suggestion that the system may "assess the security vulnerabilities of a remote computer connected to the network." Examiner points applicant to column 13, lines 1-6 of Shostack et al.: "The fourth module 88 accesses the database of security vulnerabilities 92 and assess the security vulnerabilities of a remote computer connected to the network. The fourth module 88 allows a remote computer to first connect to a network service then accepts information from the service and like the second module 76, also interrogates the service."

5. Regarding claim 4, Orchier et al. clearly teach selecting modules based on specifications of the local computer. Orchier et al. teach multiple modules according to different platforms (specifications) (Orchier et al., column 4, lines 48-67, column 5, lines 1-22).

6. Regarding claims 9 and 10, Shostack et al. teach "A sixth module is a communications module that allows the integrated security system 160 to communicate with a similar system over a computer network. The sixth module **may allow**

communication between the similar system and the various modules and software applications for sharing database files, for sharing workload in breaking long lists of passwords, transmitting reports or data for purposes of analysis, **reporting to a management station, configuring files or configuring an operating system,** and invoking a remote system to send a software enhancement. The sixth module may also include cryptographic code for protecting the confidentiality and integrity of the information being transmitted" (emphasis added). Clearly, Shostack et al. do teach two-way communication, including active feedback.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 12, 23-27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

These claims recite the limitations "wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer" and "wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters". It is unclear what is configured, the module or the execution of the modules.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-6, 9-10, 12, 15-17, 20-21, 23-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (US Patent Number: 6,298,445), and further in view of Orchier et al. (US Patent Number: 6,070,244).

Regarding claim 1, Shostack et al. teach a method of remotely detecting vulnerabilities on a local computer, comprising:

a) installing an agent on a local computer (column 11, lines 40-60);

b) receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 11, lines 5-17, column 13, lines 1-6);

c) decrypting the commands on the local computer utilizing the agent (column 11, lines 5-17, column 13, lines 1-6);

d) processing the commands on the local computer utilizing the agent (column 13, lines 1-6); and

e) performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 13, lines 1-6);

- wherein the agent includes a plurality of risk-assessment modules (column 12, lines 14-19);

- wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 12, lines 55-57);
- wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26).

Shostack et al. do not explicitly disclose wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters, but one of ordinary skill in the art at the time the invention was made would have associated parameters to commands for executing specific applications or modules (column 8, lines 42-54, "the script can include different commands and subroutines for accessing software applications..."). However, Orchier et al. teach wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to process commands by extracting parameters associated with the commands. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate automatic changes of system parameters and provide for a self-correcting data security audit system (Orchier et al., column 2, lines 35-50).

Regarding claims 4 and 15, Shostack et al. do not disclose wherein the risk-assessment modules are selected for the agent based on specifications of the local computer. However, Orchier et al. teach wherein the risk-assessment modules are

selected for the agent based on specifications of the local computer (column 4, lines 48-67, column 5, lines 1-6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to select risk-assessment modules based on specifications of the local computer. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate automatic changes of system parameters and provide for a self-correcting data security audit system (Orchier et al., column 2, lines 35-50).

Regarding claims 5 and 16, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claims 1 and 12 respectively above. Furthermore, Shostack et al. teach wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function (column 12, lines 27-40), a GETPWENT module for retrieving an entry from a password database (column 12, lines 58-67), a GETGRENT module for retrieving an entry from a group database (column 12, lines 41-57), a CHKSUM module for performing a checksum operation on a file (column 12, lines 23-34), and an EXEC module for executing a command (column 12, lines 14-20).

Regarding claims 6 and 17, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claims 1 and 12 respectively above. Furthermore, Shostack et al. teach wherein the risk-assessment modules are selected (column 12, lines 17-19) from the group consisting of a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for

returning contents of a directory, a FIND module for locating a list of files based on a given function (column 12, lines 27-40), a GETPWENT module for retrieving an entry from a password database (column 12, lines 58-67), a GETGRENT module for retrieving an entry from a group database (column 12, lines 41-57), a CHKSUM module for performing a checksum operation on a file (column 12, lines 23-34), and an EXEC module for executing a command (column 12, lines 14-20).

Regarding claims 9 and 20, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claims 1 and 12 respectively above. Furthermore, Shostack et al. teach transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network (column 13, lines 18-30, 37-44).

Regarding claims 10 and 21, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 9 and 20 respectively above. Furthermore, Orchier et al. teach receiving feedback to the results from the remote computer utilizing the network (column 7, lines 36-67).

Regarding claim 12, Shostack et al. teach a computer program product embodied on a computer readable medium for remotely detecting vulnerabilities on a local computer, comprising:

a) computer code for installing an agent on a local computer (column 11, lines 40-60);

b) computer code for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 11, lines 5-17, column 13, lines 1-6);

c) computer code for decrypting the commands on the local computer utilizing the agent (column 11, lines 5-17, column 13, lines 1-6);

d) computer code for processing the commands on the local computer utilizing the agent (column 13, lines 1-6); and

e) computer code for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 13, lines 1-6);

- wherein the agent includes a plurality of risk-assessment modules (column 12, lines 14-19);
- wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 12, lines 55-57);
- wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26).

Shostack et al. do not explicitly disclose wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters, but one of ordinary skill in the art at the time the invention was made would have associated parameters to commands for executing specific applications or modules (column 8, lines 42-54, "the script can include different commands and subroutines for

accessing software applications..."). However, Orchier et al. teach wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to process commands by extracting parameters associated with the commands. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate automatic changes of system parameters and provide for a self-correcting data security audit system (Orchier et al., column 2, lines 35-50).

Regarding claim 23, Shostack et al. teach a system for remotely detecting vulnerabilities on a local computer, comprising:

a) an agent installed on a local computer (column 11, lines 40-60) for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 11, lines 5-17, column 13, lines 1-6), decrypting the commands on the local computer (column 11, lines 5-17, column 13, lines 1-6), and processing the commands on the local computer (column 13, lines 1-6); and

b) wherein the risk-assessment scan is performed on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 13, lines 1-6);

- wherein the agent includes a plurality of risk-assessment modules (column 12, lines 14-19);

- wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 12, lines 55-57);
- wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26).

Shostack et al. do not explicitly disclose wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters, but one of ordinary skill in the art at the time the invention was made would have associated parameters to commands for executing specific applications or modules (column 8, lines 42-54, "the script can include different commands and subroutines for accessing software applications..."). However, Orchier et al. teach wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to process commands by extracting parameters associated with the commands. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate automatic changes of system parameters and provide for a self-correcting data security audit system (Orchier et al., column 2, lines 35-50).

Regarding claim 24, Shostack et al. teach a system for remotely detecting vulnerabilities on a local computer, comprising:

a) means for installing an agent on a local computer (column 11, lines 40-60);

b) means for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 11, lines 5-17, column 13, lines 1-6);

c) means for decrypting the commands on the local computer utilizing the agent (column 11, lines 5-17, column 13, lines 1-6);

d) means for processing the commands on the local computer utilizing the agent (column 13, lines 1-6); and

e) means for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 13, lines 1-6);

- wherein the agent includes a plurality of risk-assessment modules (column 12, lines 14-19);
- wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 12, lines 55-57);
- wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26).

Shostack et al. do not explicitly disclose wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters, but one of ordinary skill in the art at the time the invention was made would have associated parameters to commands for executing specific applications or modules (column 8, lines 42-54, "the script can include different commands and subroutines for

accessing software applications..."). However, Orchier et al. teach wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to process commands by extracting parameters associated with the commands. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate automatic changes of system parameters and provide for a self-correcting data security audit system (Orchier et al., column 2, lines 35-50).

Regarding claims 25 and 26, Shostack et al. teach remotely detecting vulnerabilities from a remote computer, comprising:

a) sending encrypted commands from a remote computer to an agent on a local computer for executing a risk-assessment scan utilizing a network (column 11, lines 5-17, column 13, lines 1-6) , the commands adapted for being decrypted (column 11, lines 5-17, column 13, lines 1-6) and processed on the local computer (column 13, lines 1-6) utilizing the agent for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 13, lines 1-6);

b) receiving results of the risk-assessment scan from the local computer utilizing the network (column 13, lines 18-30, 37-44); and

- wherein the agent includes a plurality of risk-assessment modules (column 12, lines 14-19);

- wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 12, lines 55-57);
- wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26).

Shostack et al. do not explicitly disclose c) transmitting feedback to the results from the remote computer to the local computer utilizing the network; nor wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters, but one of ordinary skill in the art at the time the invention was made would have associated parameters to commands for executing specific applications or modules (column 8, lines 42-54, "the script can include different commands and subroutines for accessing software applications..."). However, Orchier et al. teach c) transmitting feedback to the results from the remote computer to the local computer utilizing the network (column 7, lines 36-67); and wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to process commands by extracting parameters associated with the commands. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate automatic changes of system parameters and provide for a self-correcting data security audit system (Orchier et al., column 2, lines 35-50).

Regarding claim 27, Shostack et al. teach remotely detecting vulnerabilities on a local computer, comprising:

a) installing an agent on a local computer (column 11, lines 40-60), the agent including a plurality of risk-assessment modules (column 12, lines 14-19) selected based on at least one aspect of the computer;

b) receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 11, lines 5-17, column 13, lines 1-6);

c) decrypting the commands on the local computer utilizing the agent (column 11, lines 5-17, column 13, lines 1-6);

d) authenticating the commands on the local computer utilizing the agent (column 13, lines 7-17);

e) processing the commands on the local computer utilizing the agent (column 13, lines 1-6), the commands adapted to execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 12, lines 55-57); and

f) performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 13, lines 1-6);

g) transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network (column 13, lines 18-30, 37-44);

- wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26);

Shostack et al. do not explicitly disclose h) receiving feedback to the results from the remote computer utilizing the network; nor wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters, but one of ordinary skill in the art at the time the invention was made would have associated parameters to commands for executing specific applications or modules (column 8, lines 42-54, "the script can include different commands and subroutines for accessing software applications..."). However, Orchier et al. teach h) receiving feedback to the results from the remote computer utilizing the network (column 7, lines 36-67); and wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to process commands by extracting parameters associated with the commands. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate automatic changes of system parameters and provide for a self-correcting data security audit system (Orchier et al., column 2, lines 35-50).

Regarding claim 28, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 10 above. Furthermore, Orchier et al. teach wherein the feedback is active (column 7, lines 36-67).

Regarding claim 29, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 28 above. Furthermore, Orchier et al. teach

wherein the feedback includes additional commands and additional modules for correcting the vulnerabilities in response to the additional commands (column 7, lines 36-67).

Regarding claim 30, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 10 above. Furthermore, Shostack et al. teach wherein the feedback is passive (column 13, lines 36-44).

Regarding claim 31, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 30 above. Furthermore, Shostack et al. disclose wherein the feedback includes descriptions as to how to correct the vulnerabilities (column 4, lines 8-12, column 13, lines 36-44). Having a database of security vulnerabilities and the ability to generate a report log of the security vulnerabilities found, it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a log that includes how to correct the vulnerabilities.

Regarding claim 32, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 9 above. Furthermore, Shostack et al. teach wherein the results include a log of the risk-assessment scan (column 13, lines 39-44).

Regarding claim 33, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 32 above. Furthermore, Shostack et al. teach wherein the results include an identification of the vulnerabilities (column 13, lines 39-44).

Regarding claim 34, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 1 above. Furthermore, Shostack et al. teach

wherein a plurality of the commands are each associated with only one of the risk-assessment modules (column 12, lines 14-26).

Regarding claim 35, the combination of Shostack et al. and Orchier et al. teaches the limitations as set forth under claim 1 above. Furthermore, Orchier et al. teach wherein a different set of risk-assessment modules exists on different local computers, based on a platform associated with each of the local computers (column 4, lines 48-62).

Claims 11, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. and Orchier et al. as applied to claim 1, 12 respectively above, and further in view of Smid et al. (US Patent Number: 4,386,233).

Regarding claims 11 and 22, Shostack et al. and Orchier et al. do not disclose expressly wherein the commands are decrypted utilizing a shared key. However, Smid et al. teach wherein the commands are decrypted utilizing a shared key (column 3, lines 5-12). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decrypt commands utilizing a shared key. One of ordinary skill in the art would have been motivated to perform such a modification to authenticate access (Smid et al., column 2, lines 60-68).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100